(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01799 A2

(51) International Patent Classification[7]: H04L 12/18, 29/06

(21) International Application Number: PCT/US01/20181

(22) International Filing Date: 26 June 2001 (26.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/603,079 26 June 2000 (26.06.2000) US

(71) Applicant: CONVERA CORPORATION [US/US]; 1921 Gallows Road, Suite 200, Vienna, VA 22182 (US).

(72) Inventor: ROZAS, Carlos, V.; 1534 NW Morgan Lane, Portland, OR 97229 (US).

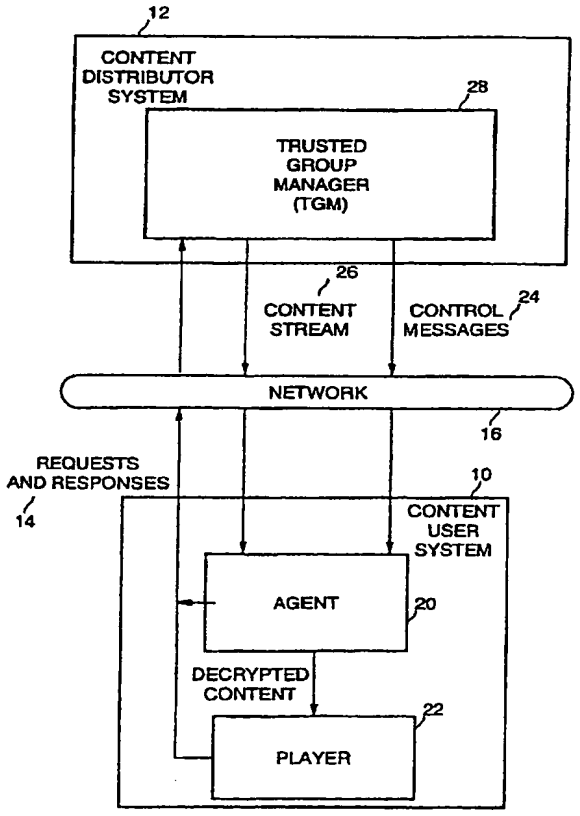
(74) Agents: TALBOT, C., Scott et al.; Cooley Godward LLP, Patent Group, One Freedom Square-Reston Town Center, 11951 Freedom Drive, Reston, VA 20190-5601 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURELY MANAGING MEMBERSHIP IN GROUP COMMUNICATIONS



(57) Abstract: Managing group membership of receivers-in-broadcast and multicast content distribution systems. The invention provides for security in group communications where a single source is broadcasting or multicasting to multiple destination points on a network such as the Internet using a local agent resident on a user system, an authorization token, and a trusted group manager (TGM) representing a content distributor. The local agent may be tamper resistant code providing support for key agreement, decryption, and message authentication functions. The authorization token describes which agents are active and available to decrypt digital content or a per packet basis. The TGM establishes a session key with a group of local agents and generates authorization tokens. The local agent adds and removes itself from a content distribution session (and associated group) based on a series of protocols that do not require a "re-key" for an encrypted content stream being broadcast or multicast by a content distributor. The protocols include operations for registering with a group, joining a group, and leaving a group.

WO 02/01799 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR SECURELY MANAGING MEMBERSHIP IN GROUP COMMUNICATIONS

BACKGROUND

1. FIELD

The present invention relates generally to content protection in multicast and broadcast communications systems and, more specifically, to providing security for digital content communicated to multiple group members.

2. DESCRIPTION

Physical objects such as compact disks (CDs) or cassette tapes holding entertainment content provide some measure of their own security simply by virtue of the fact that playback of the content is tied to having the physical object present. If one makes a copy (such as by recording music from a CD onto a cassette tape), the quality of the content is degraded. If one wants the highest quality content, one must buy or otherwise obtain an original product. The content distribution industry made it convenient for customers or users to have access to content by making it widely available at high-traffic consumer locations such as record and video stores, malls, and major discount stores. Presently, business to consumer electronic commerce, especially in the area of entertainment content, is growing rapidly on the World Wide Web (WWW) of the Internet. The proliferation of connected personal computers (PCs) and other Internet access devices, the growing bandwidth of the Internet, and better compression techniques are making it possible for content owners to take advantage of the Web as a place to offer digital content for sale and distribution. Many businesses are also increasingly using the Internet as a means to distribute confidential documents, images, video presentations, training and other digital content to employees at geographically dispersed locations.

Thus, the distribution of digital content over the Internet is increasing. With the increasing use of the Internet to buy, sell, or send music, video, documents, images, and other copyrighted or confidential content in digital form, comes the need to protect that content from unauthorized use.

One mechanism to distribute digital content is through broadcast or multicast means. In this type of application, a content distributor (e.g., a broadcaster) distributes the content to multiple users over a network such as the Internet. In some instances, the content may be distributed in a temporal manner, such as the streaming of a movie or a music concert to a group of viewers, for example. This is one example of a growing number of digital content communications applications that require group management capabilities. Group management typically includes ensuring that only authorized (e.g., paying) users can be a member of a group, excluding past group members from viewing current content, and excluding new group members from viewing old content. The traditional mechanism for providing group management features is to encrypt the data stream carrying the content and to perform a "re-key" when the group membership changes (e.g., when users join or leave the group). This involves distributing a new secret (e.g., the new decryption key) to all current and authorized members of the group. This approach has at least two drawbacks. It is computationally expensive, potentially involving up to O(n) public key operations for every re-key attempt. It also typically requires the buffering or dropping of content packets during the delivery of the new key.

Hence, new approaches to securely managing groups that avoid the disadvantages of the prior art are desired.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram of a group management and content protection system according to an embodiment of the present invention;

Figure 2 is a flow diagram illustrating register group member processing according to an embodiment of the present invention;

Figure 3 is a flow diagram illustrating join processing according to an embodiment of the present invention;

Figure 4 is a flow diagram illustrating application message processing according to an embodiment of the present invention;

Figure 5 is a flow diagram illustrating leave processing according to an embodiment of the present invention; and

Figure 6 is a diagram illustrating an exemplary system used by a content distributor or a content user according to an embodiment of the present invention.

DETAILED DESCRIPTION

An embodiment of the present invention is a method and apparatus for managing group membership in broadcast and multicast content distribution systems. The present invention provides for security in group communications where a single source is broadcasting or multicasting to multiple destination points on a network such as the Internet. An embodiment of the present invention comprises a local agent resident on a user system, an authorization token, and a trusted group manager (TGM) representing a content distributor. The local agent may be tamper resistant code providing support for key agreement, decryption, and message authentication functions. The authorization token describes which agents are active and available to decrypt digital content. In one embodiment, the digital content may be decrypted and accessed on a per packet basis. In other embodiments, other units of digital content may be processed according to the present invention. The TGM establishes a session key with a group of local agents and generates authorization tokens. In one embodiment, the local agent adds and removes itself from a content distribution session (and associated group) based on a series of protocols that do not require a "re-key" for an encrypted content stream being broadcast or multicast by a content distributor. The protocols include operations for registering with a group, joining a group, and leaving a group. The protocol details depend on the nature of the authorization code. In one embodiment, the authorization token includes a list of all active agents.

Reference in the specification to "one embodiment" or "an embodiment" of the present invention means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrase "in one embodiment" appearing in various places throughout the specification are not necessarily all referring to the same embodiment.

A content creator is an entity that authors digital content. The content creator generates the digital content data, which may be stored in a file within a storage medium on a computer system or other digital processing system and subsequently broadcast or multicast to a plurality of content users over a network. For example, a content creator may record and mix music in a recording studio, or film a movie, and then store the created content in a digital form for future transmission or distribution. In another example, the content may be a corporate presentation to employees, shareholders, customers, etc. The content may be any multimedia content in a digital form, such as audio, video, images, text, music, movies, books, or other data. The content may be sent to one or more users in a continuous stream of content data. The format of the content may vary widely depending on the type of content. It is assumed that the content is created in a trusted environment.

A content distributor system is an entity that sells or distributes the content over a communications medium such as the Internet or other network. The content distributor system may be controlled by the content owner or may be an authorized independent distributor or reseller of the content. The content distributor system may be implemented and managed by a broadcaster or multicaster. Where the content is digitized music, the content distributor system may represent a music or record company that owns rights to the music or an authorized distributor, such as an on-line retailer. Where the content is digitized film, the content distributor system may represent a movie company that owns the rights to the movie or an authorized distributor such as a broadcasting network. The content distributor system may use one or more server systems to distribute the content to one or more users on demand.

Figure 1 is a diagram of a group management and content protection system according to an embodiment of the present invention. A content user system 10 is an entity that obtains and consumes content distributed by a content distributor system 12. The content user represents any party seeking to process digital content provided -by content distributor system 12, including individual end users, businesses, and other organizations. Content user system 10 operates as a client in a client/server operating model in conjunction with a server (not shown) operated by content distributor system 12. The content user system sends requests for resources (e.g., Web pages, content) and responses to earlier queries 14 to the content distributor system over a network 16

(such as the Internet) and receives data in response to the requests. Network 16 may be any network or series of interconnected networks capable of transporting digital content from the content distributor system to one or more content user systems. For example, network 16 may be a local area network (LAN), a wide area network (WAN), the Internet, a wireless network, or a terrestrial broadcast network such as a satellite communications network. In one embodiment, the content user system 10 comprises at least one of a personal computer (PC) system, an Internet appliance, a set-top box, a handheld computer, a personal digital assistant (PDA), or other computing device. In a multicast or broadcast environment, there may be many content user systems receiving content from a single content distributor system.

According to embodiments of the present invention, the content user system includes components resident therein to control secure reception and playback of content received from content distributor system 12. The content user system evaluates content requirements for authorized playback and system characteristics to determine if the content user system and its components may be trusted. The content user system includes one or more unique, trusted software components that represent the interests of the content creator or content distributor. This software component, called an agent, acts a custodian of the content creator's interests. In one embodiment, the agent 20 establishes itself as trusted via known tamper-resistant technologies and continuous integrity checking. It then extends the perimeter of trust by continuously checking the integrity of other software components such as player 22. Because of this, attempts to tamper with the player or the agent may be detected by the agent 20, and further playback of content by player 22 may be halted. In another embodiment, the agent may operate in an isolated execution mode that provides a measure of security to deter tampering with the agent. In other embodiments, other methods for protecting the agent from tampering may be employed.

The agent validates- and enforces the conditions that must be fulfilled before the content can be consumed or rendered. These conditions can be anything that the content distributor chooses, consistent with the goal of balancing the protection of the content distributor's rights and the desire to give the content user a satisfying experience in obtaining and rendering the content. For example, the agent might check the content user system 10 for an electronic copy of a purchase receipt or verify a

player identifier (ID) or user password. There may be many conditions an agent might verify on the content user system before allowing decryption and rendering of content to occur. After the agent has determined that the legitimate conditions for content usage have been met, the agent decrypts the content so the content may be rendered by the player. In one embodiment, decryption of the content may be allowed only if the agent is an authorized member of a group associated with a content stream. To reduce the incentive for hacking attempts and to minimize the amount of content that is protected by the same security mechanism, the agent may in some embodiments be repeatedly renewed.

Thus, agent 20 interacts with player 22, acting as a controller to determine if and when the content that is received from the content distributor may be rendered. Player 22 may be any software component or application for processing of digital content. Processing may include storing, transferring, displaying, or otherwise rendering the content. Player 22 may employ various other software components and plug-ins (not shown) in order to process the content, including codecs to decode and decompress the decrypted content.

The agent controls the player's access to the content according to control messages 24 received by the agent from the content distributor system via the network. The control messages may or may not be included in a content stream 26. The content stream primarily comprises requested content. However, these two data flows are shown separately in Figure 1 for reasons of clarity. Trusted group manager (TGM) 28 may be a component within a content distributor system that handles processing for registering, joining and leaving a group for a particular content stream.

Before access to a particular content stream is allowed, a content user system registers as a possible group member for the content stream with the TGM. That is, the agent registers itself with the TGM, or another software component resident on the content user system registers the agent with the TGM. In some embodiments, the agent does not initiate or control the registration protocol, but another software component (not shown) on the content user system that interacts with the user, the agent, and the TGM may control the registration process. This client-side software component may begin the protocol after the user selects a particular content stream he or she is interested in joining. The client-side software component may then retrieve a content

stream identifier, a transaction identifier associated with the upcoming usage of the content stream, and the agent's credentials. An agent identifier may be included in the agent's credentials. The transaction identifier allows the TGM to determine if the user has the right to access the content stream. This abstraction allows for the idea that some commerce-like event has occurred. The agent credentials let the TGM determine if the agent is capable of controlling access to the content stream. If it determines that the agent is not capable, the TGM may provide an updated agent to the content user system.

Figure 2 is a flow diagram illustrating register group member processing according to an embodiment of the present invention. At block 50, the agent or the client-side software component, depending on the embodiment, sends the agent's credentials, an identifier (ID) of the selected content stream, and an agent identifier in a request message 14 to the TGM. At block 52, the TGM verifies the agent's credentials received in the request message. Some authentication indicators included in the credential may be the source of the agent, freshness or age of the agent, capabilities of the agent, and so on. At block 54, the TGM verifies the agent and the content stream. This verification may include checking billing information associated with the agent's user, ensuring that the content stream ID is valid and scheduled for broadcast or multicast, and other checks.

At block 56, the TGM generates a registration token for the agent and the selected content stream. In one embodiment, the registration token comprises an initial nonce, the content stream ID (which is preferably is unique) for the content requested by the agent, and a session key. In one embodiment, the nonce may be a counter that allows the TGM to track what privileges are being granted to the agent. The nonce may be a unique string of values to identify a particular transaction. The session key may be a cryptographic key used by the agent to decrypt received content that has been encrypted by the content distributor system according to well-known methods in either symmetric key or asymmetric key cryptography. The session key may be associated with a particular. group of users being allowed access to a particular content stream. The user of the content user system may know the content stream ID, but the session key should be hidden from the user by encrypting the initial nonce and the session key within the registration token. In one embodiment, the key to decrypt the initial nonce

and the session key may be included in the registration token to be decrypted by logic within the tamper resistant agent. At block 58, the TGM sends the registration token to the agent in a control message 24.

Thus, the registration function establishes a session key between the TGM and the agent of the user for a particular content stream. The session 'key may be identical for all group members for the group associated with the content stream and may be used to decrypt application messages sent by the TGM to the group members. Before providing the session key, the TGM authenticates the agent's credentials to verify it is trusted not to divulge the session key to anyone, including the user. The registration function may be performed at any time prior to joining a group.

Once a user is registered for a group, the user must join the group in order to receive access to the content stream. The join function notifies the TGM that the user wishes to join the content streaming session at the current time. The TGM, upon verifying that the user is registered, adds the user's agent to an authorized agent list for the selected content stream. Figure 3 is a flow diagram illustrating join processing according to an embodiment of the present invention. At block 70, the agent sends a join message to the TGM. In one embodiment, the join message comprises an ID of the requesting user, the content stream ID, and a cryptographic hash of a join command or keyword, the user ID, the nonce received during registration processing, and the content stream ID. In one embodiment, the user ID and the content stream ID may be sent in the clear to the TGM. At block 72, the TGM verifies the join message parameters according to information known by the TGM. Given the user ID and the content stream ID, the TGM can recover the nonce created during registration processing for this user from a database or other storage accessible to the TGM. With the nonce, the TGM can recreate the join message and validate the contents of the message. In this embodiment, the nonce should be kept secret. In other embodiments where the session key is included, the nonce may not need to be kept secret. If the received and recreated join messages match, at block 74 the TGM adds the user's agent identifier to an authorized agents list for the selected content stream.

Once the user has joined the group having access to the content stream, the TGM can now send control messages to the user's agent. The control message may be included in packets within the content stream. The TGM broadcasts or multicasts

packets to group members and possibly others who are not currently valid group members. There may be two types of packets communicated over the network. The first packet type comprises a content stream packet. A content stream packet comprises a message ID and a message. The message comprises the content. The content stream packet is encrypted by the TGM with the session key communicated to the agent during registration processing. The second type of packet comprises a control packet. In one embodiment, a control packet comprises two components. The first component may be a cryptographic hash of the session key, the authorization token, and the session key. The second component may be the authorization token. In one embodiment, the hash comprises a relatively small number of bits, such as approximately 128 bits or 160 bits. The authorization token comprises at least the message ID and the authorized agents list. Thus the authorization token is bound to the content stream packet. The authorized agents list comprises a data structure comprising the IDs of the currently active or authorized agents.

When the agent receives a stream of packets from the TGM, the agent reads the packets and determines what to do with them. Figure 4 is a flow diagram illustrating application message processing according to an embodiment of the present invention. Upon receiving a control packet and a corresponding content packet at block 90, the agent then performs a series of verifications. At block 92, the agent verifies the authorization token received in the control packet by computing the hash of the token and the session key. To compute the hash the agent uses the authorization token received in the control packet and the session key received during registration processing. If the recomputed hash matches the hash in the control packet, then at block 94 the agent determines if the message ID from the content packet matches the message ID in the authorization token in the control packet. If they match, the control packet corresponds to the content packet. In some embodiments, the agent may decrypt the message ID, if necessary, using the session key. Next, at block 96 the agent determines if the authorized agents list in the authorization token from the control packet includes the ID of the agent. If any of the above checks fail, then further error processing may be performed, such as the termination of the agent and the player. If all of the above checks are successful, the agent at block 98 decrypts the message in the content packet using the session key to obtain the content. The content in the message

may then be processed by the player, such as by rendering, storage, display, or further transmission of the content.

The process of receiving control and content packets may be repeated for all or some of the packets in the content stream. At some point, a user may desire to terminate participation in the session. This termination may even be before the scheduled end of the session. To leave an active session, the agent sends a leave message to the TGM. Figure 5 is a flow diagram illustrating leave processing according to an embodiment of the present invention. At block 100, the agent or another client-side software component generates and sends a leave message to the TGM. In one embodiment, the leave message comprises a hash of a leave command or keyword, the ID of the user, the nonce received during registration, a transaction ID, and the content stream ID. The leave message may also include the content stream ID (unencrypted). At block 102, the TGM verifies the parameters of the leave message. For example, the TGM may use the nonce to validate that the leave message came from a previously registered user. At block 104, the TGM deletes the agent associated with the user ID from the authorized agents list for the content stream identified by the content stream ID if the leave parameters are valid. Subsequently, the user's agent will not be able to decrypt the content packets for the content stream because the agent will not be included in the authorized agents list within the authorization token.

Hence, the present invention allows a trusted group manager (TGM) to manage groups for communications of digital content. The TGM has control over who is currently an authorized user for a particular session of streaming content over a network without re-keying all group members. With the present invention, re-key operations are no longer required for the purpose of managing group membership, but may be used only if the underlying cryptographic cipher needs re-keying to maintain adequate security. The present system is more flexible than prior approaches and provides application level security. Registration of a user may occur far in advance of the actual content streaming session. The present invention provides strong forward and backward security. Backward security relates to preventing a user who joins the session at a particular point in time from accessing past content streamed before the point in time. Forward security relates to preventing a user who leaves a session at a

point in time from continuing to access subsequently streamed content after that point in time.

In other embodiments, other authorization protocols may be employed to improve the scalability of the present invention. For example, a system designer may use chaining between authorization tokens to describe only the differences of authorized agents lists, between packets. A system designer may use a hierarchical model that employs trusted local agent intermediaries to manage authorization tokens "locally" (e.g., for a LAN). A system designer may use an exclusion list to provide only forward secrecy depending on system requirements.

In another variation, the join protocol may be augmented to provide only backwards secrecy by requiring the local agent to only decrypt new packets. This may avoid the need for per packet authorization tokens. In this embodiment, the TGM generates an authorization packet for the agent. The authorization packet comprises of a hash and an authorization token. The authorization token comprises a message having a message ID and an agent ID. The hash is a result of hashing the session key, authorization token, and the session key. Upon receiving the authorization packet, the agent checks the validity of the authorization token by recreating the hash and verifying that it matches the hash in the authorization packet.

Upon receiving any content packet, the agent uses a function F which, given the content message ID and the message ID in the authorization token, returns a Boolean answer to whether or not the agent can decrypt the content packet. One embodiment of function F may compare the two IDs and if the content message ID is greater than the authorization token message ID, then F returns TRUE and the agent decrypts the content packet.

In other embodiments, instead of generating multiple hashes, several of the messages may be encrypted (e.g., the TGM encrypts the authorization packet using a derivative of the session key; for example, the TGM applies a function G to the session key s to generate a new key s' which is used to encrypt the authorization packet s'=G(s)).

In the preceding description, various aspects of the present invention have been described. For purposes of explanation, specific numbers, systems and configurations were set forth in order to provide a thorough understanding of the present invention.

However, it is apparent to one skilled in the art having the benefit of this disclosure that the present invention may be practiced without the specific details. In other instances, well-known features were omitted or simplified in order not to obscure the present invention.

Embodiments of the present invention may be implemented in hardware or software, or a combination of both. However, embodiments of the invention may be implemented as computer programs executing on programmable systems comprising at least one processor, a data storage system (including volatile and non-volatile memory and/or storage elements), at least one input device, and at least one output device. Program code may be applied to input data to perform the functions described herein and generate output information. The output information may be applied to one or more output devices, in known fashion. For purposes of this application, a processing system embodying the group management functions includes any system that has a processor, such as, for example, a digital signal processor (DSP), a microcontroller, an application specific integrated circuit (ASIC), or a microprocessor.

The programs may be implemented in a high level procedural or object oriented programming language to communicate with a processing system. The programs may also be implemented in assembly or machine language, if desired. In fact, the invention is not limited in scope to any particular programming language. In any case, the language may be a compiled or interpreted language.

The programs may be stored on a removable storage media or device (e.g., floppy disk drive, read only memory (ROM), CD-ROM device, flash memory device, digital versatile disk (DVD), or other storage device) readable by a general or special purpose programmable processing system, for configuring and operating the processing system when the storage media or device is read by the processing system to perform the procedures described herein. Embodiments of the invention may also be considered to be implemented as a machine-readable storage medium, configured for use with a processing system, where the storage medium so configured causes the processing system to operate in a specific and predefined manner to perform the functions described herein.

An example of one such type of processing system is shown in Figure 6, however, other systems may also be used and not all components of the system shown

are required for the present invention. Sample system 400 may be used, for example, to execute the processing for embodiments of the key hierarchy and content protection system, in accordance with the present invention, such as the embodiment described herein. Sample system 400 is representative of processing systems based on the PENTIUM®II, PENTIUM® III, and CELERONT™ microprocessors available from Intel Corporation, although other systems (including personal computers (PCs) having other microprocessors, engineering workstations, other set-top boxes, and the like) and architectures may also be used.

Figure 6 is a block diagram of a system 400 of one embodiment of the present invention. The system 400 includes a processor 402 that processes data signals. Processor 402 may be coupled to a processor bus 404 that transmits data signals between processor 402 and other components in the system 400.

System 400 includes a memory 406. Memory 406 may store instructions and/or data represented by data signals that may be executed by processor 402. The instructions and/or data may comprise code for performing any and/or all of the techniques of the present invention. Memory 406 may also contain additional software and/or data (not shown). A cache memory 408 may reside inside processor 402 that stores data signals stored in memory 406.

A bridge/memory controller 410 may be coupled to the processor bus 404 and memory 406. The bridge/memory controller 410 directs data signals between processor 402, memory 406, and other components in the system 400 and bridges the data signals between processor bus 404, memory 406, and a first input/output (I/O) bus 412. In this embodiment, graphics controller 413 interfaces to a display device (not shown) for displaying images rendered or otherwise processed by the graphics controller 413 to a user.

First I/O bus 412 may comprise a single bus or a combination of multiple buses. First I/O bus 412 provides communication links between components in system 400. A network controller 414 may be coupled to the first I/O bus 412. In some embodiments, a display device controller 416 may be coupled to the first I/O bus 412. The display device controller 416 allows coupling of a display device to system 400 and acts as an interface between a display device (not shown) and the system. The display device

receives data signals from processor 402 through display device controller 416 and displays information contained in the data signals to a user of system 400.

A second I/O bus 420 may comprise a single bus or a combination of multiple buses. The second I/O bus 420 provides communication links between components in system 400. A data storage device 422 may be coupled to the second I/O bus 420. A keyboard interface 424 may be coupled to the second I/O bus 420. A user input interface 425 may be coupled to the second I/O bus 420. The user input interface may be coupled to a user input device, such as a remote control, mouse, joystick, or trackball, for example, to provide input data to the computer system. An audio controller 427 may be coupled to the second I/O bus for handling processing of audio signals through one or more loudspeakers (not shown). A bus bridge 428 couples first I/O bridge 412 to second I/O bridge 420.

Embodiments of the present invention are related to the use of the system 400 as a content distributor or content user system. According to one embodiment, such processing may be performed by the system 400 in response to processor 402 executing sequences of instructions in memory 404. Such instructions may be read into memory 404 from another computer-readable medium, such as data storage device 422, or from another source via the network controller 414, for example. Execution of the sequences of instructions causes processor 402 to execute group management and content protection processing according to embodiments of the present invention. In an alternative embodiment, hardware circuitry may be used in place of or in combination with software instructions to implement embodiments of the present invention. Thus, the present invention is not limited to any specific combination of hardware circuitry and software.

The elements of system 400 perform their conventional functions in a manner well known in the art. In particular, data storage device 422 may be used to provide long-term storage for the executable instructions and data structures for embodiments of the group management and content protection system in accordance with the present invention, whereas memory 406 is used to store on a shorter term basis the executable instructions of embodiments of the group management and content protection system in accordance with the present invention during execution by processor 402.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the inventions pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method of securely managing membership in a group of authorized users, the group being associated with a session for receiving a content stream comprising:

registering an agent representing a user with a trusted group manager of a distributor of the content stream; and

joining, by the agent, as a member of the group for authorized access to the content stream.

2. The method of claim 1, further comprising receiving packets of the content stream by the agent and processing the packets by the agent to access the content when the agent is a member of the group.

3. The method of claim 2, wherein packets of the content stream are encrypted with a first key by the distributor prior to communication to group members and further comprising decrypting packets of the content stream to obtain the content by the agent after joining the group, without encrypting the content stream by the distributor with a second key different than the first key.

4. The method of claim 1, wherein the agent comprises tamper resistant software.

5. The method of claim 1, further comprising the agent leaving the group thereby preventing subsequent access to content of the content stream by the agent.

6. The method of claim 5, wherein packets of the content stream are encrypted with a first key by the distributor prior to the communication to group members and further comprising decrypting packets of the content stream to obtain the content by other group members after the agent leaves the group, without encrypting the content stream by the distributor with a second key different than the first key.

7. The method of claim 2, wherein the packets comprise at least one content packet and at least one control packet, the at least one content packet comprising the content in encrypted form, and the at least one control packet comprising an authorization token including at least a list of identifiers of authorized agents, the list including an identifier of the agent.

8. The method of claim 7, wherein processing the packets comprises verifying integrity of the authorization token, verifying that the agent's identifier is in the authorized agents list, and decrypting the content in the at least one content packet using a session key when the integrity of the authorization token is verified and the agent identifier is in the authorized agents list.

9. The method of claim 8, wherein the at least one content packet comprises a first message identifier, the authorization token in the at least one control packet comprises a second message identifier, and wherein processing the packets further comprises matching the at least one content packet to the at least one control packet by verifying that the first message identifier matches the second message identifier.

10. The method of claim 1, wherein registering the agent comprises:

sending agent information to the trusted group manager;

verifying the agent information;

generating a registration token, the registration token including at least one of a nonce, a content stream identifier, and a session key used for decryption of the content; and

sending the registration token to the agent.

11. The method of claim 10, wherein the agent information comprises at least one of the agent's credentials, the content stream identifier, and the identifier of the agent.

12. The method of claim 1, wherein joining the group comprises adding an identifier of the agent to an authorized agents list.

13. The method of claim 5, wherein leaving the group comprises deleting an identifier of the agent from an authorized agents list.

14. An article comprising: a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for securely managing membership in a group of authorized users, the group being associated with a session for receiving a content stream, the instructions for registering an agent representing a user with a trusted group manager of a distributor of the content stream; and joining, by the agent, as a member of the group for authorized access to the content stream.

15. The article of claim 14, further comprising instructions for receiving packets of the content stream by the agent and instructions for processing the packets by the agent to access the content when the agent is a member of the group.

16. The article of claim 15, wherein packets of the content stream are encrypted with a first key by the distributor prior to communication to group members and further comprising instructions for decrypting packets of the content stream to obtain the content by the agent after joining the group, without encrypting the content stream by the distributor with a second key different than the first key.

17. The article of claim 14, wherein the agent comprises tamper resistant software.

18. The article of claim 14, further comprising the agent leaving the group thereby preventing subsequent access to content of the content stream by the agent.

19. The article of claim 18, wherein packets of the content stream are encrypted with a first key by the distributor prior to the communication to group members and further comprising instructions for decrypting packets of the content stream to obtain the content by other group members after the agent leaves the group, without encrypting the content stream by the distributor with a second key different than the first key.

20. The article of claim 15, wherein the packets comprise at least one content packet and at least one control packet, the at least one content packet comprising the content in encrypted form, and the at least one control packet comprising an authorization token including at least a list of identifiers of authorized agents, the list including an identifier of the agent.

21. The article of claim 20, wherein instructions for processing the packets comprise instructions for verifying integrity of the authorization token, verifying that the agent's identifier is in the authorized agents list, and decrypting the content in the at least one content packet using a session key when the integrity of the authorization token is verified and the agent identifier is in the authorized agents list.

22. The article of claim 21, wherein the at least one content packet comprises a first message identifier, the authorization token in the at least one control packet comprises a second message identifier, and wherein instructions for processing the packets further comprise instructions for matching the at least one content packet to the at least one control packet by verifying that the first message identifier matches the second message identifier.

23. The article of claim 14, wherein instructions for registering the agent comprise instructions for: sending agent information to the trusted group manager; verifying the agent information; generating a registration token, the registration token including at least one of a nonce, a content stream identifier, and a session key used for decryption of the content; and sending the registration token to the agent.

24. The article of claim 23, wherein the agent information comprises at least one of the agent's credentials, the content stream identifier, and the identifier of the agent.

25. The article of claim 14, wherein instructions for joining the group comprise instructions for adding an identifier of the agent to an authorized agents list.

26. The article of claim 18, wherein instructions for leaving the group comprise instructions for deleting an identifier of the agent from an authorized agents list.

27. A system for securely managing membership in a group of authorized users, the group being associated with a session for receiving a content stream over a network, the system comprising:

a trusted group manager coupled to the network to manage a list of agents authorized for access to the content stream and to distribute the content stream to group members; and

at least one agent coupled to the network to register the agent representing a user with the trusted group manager, to join as a member of the group for authorized access to the content stream, and to receive and decrypt packets of the content stream when the agent is in the list of authorized agents.

28. The system of claim 27, further comprising a player application coupled to the agent to render the decrypted packets of the content stream.

29. The system of claim 27, wherein the at least one agent receives packets of the content stream and processes the packets to access the content when the agent is a member of the group.

30. The system of claim 29, wherein the trusted group manager encrypts packets of the content stream with a first key prior to communication to group members and the agent decrypts packets of the content stream to obtain the content after joining the group, without the trusted group manager encrypting the content stream with a second key different than the first key.

31. The system of claim 27, wherein the at least one agent comprises tamper resistant software.

32. The system of claim 27, wherein the at least one agent leaves the group thereby preventing subsequent access to content of the content stream by the at least one agent.

33. The system of claim 32, wherein the trusted group manager-encrypts packets of the content stream with a first key prior to the communication to group members and other group members decrypt packets of the content stream to obtain the

content after the at least one agent leaves the group, without the trusted group manager encrypting the content stream with a second key different than the first key.

34. The system of claim 28, wherein the packets comprise at least one content packet and at least one control packet, the at least one content packet comprising the content in encrypted form, and the at least one control packet comprising an authorization token including at least a list of identifiers of authorized agents, the list including an identifier of the agent.

35. The system of claim 34, wherein the at least one agent processes the packets to verify integrity of the authorization token, to verify that the at least one agent's identifier is in the authorized agents list, and to decrypt the content in the at least one content packet using a session key when the integrity of the authorization token is verified and the at least one agent's identifier is in the authorized agents list.

36. The system of claim 35, wherein the at least one content packet comprises a first message identifier, the authorization token in the at least one control packet comprises a second message identifier, and wherein the at least one agent processes the packets to match the at least one content packet to the at least one control packet by verifying that the first message identifier matches the second message identifier.

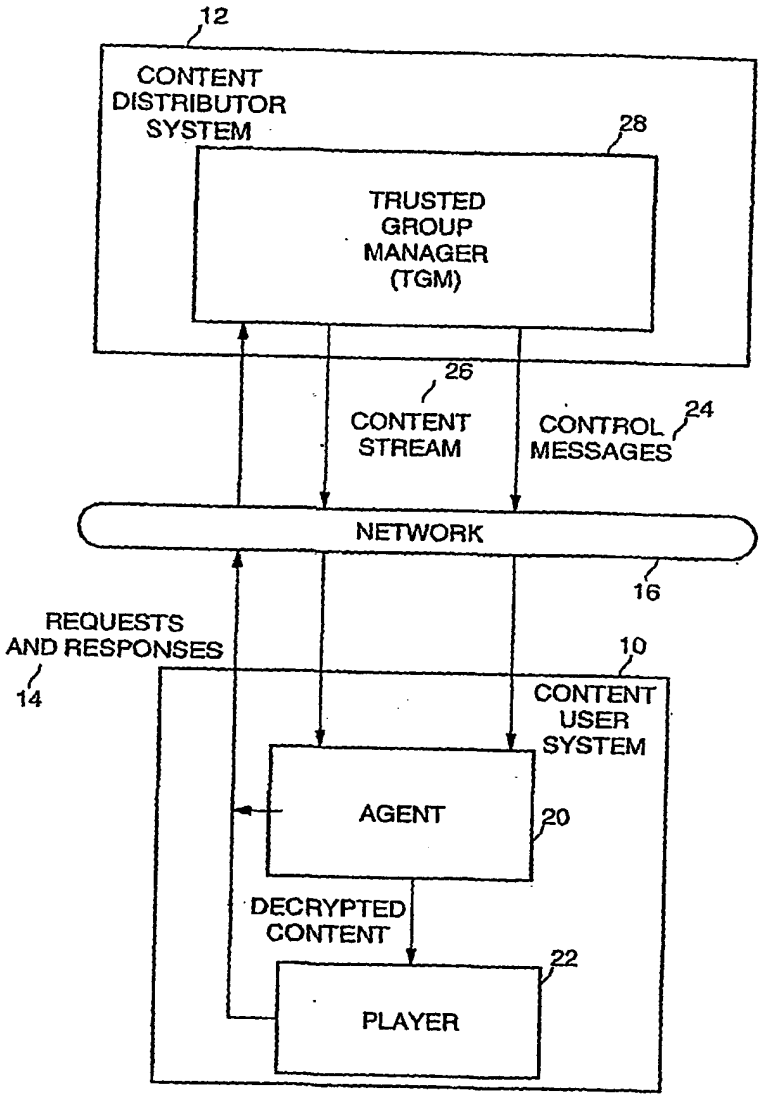

12
CONTENT DISTRIBUTOR SYSTEM
28
TRUSTED GROUP MANAGER (TGM)
26
CONTENT STREAM
CONTROL MESSAGES
24
NETWORK
16
REQUESTS AND RESPONSES
14
10
CONTENT USER SYSTEM
AGENT
20
DECRYPTED CONTENT
22
PLAYER

Figure 1

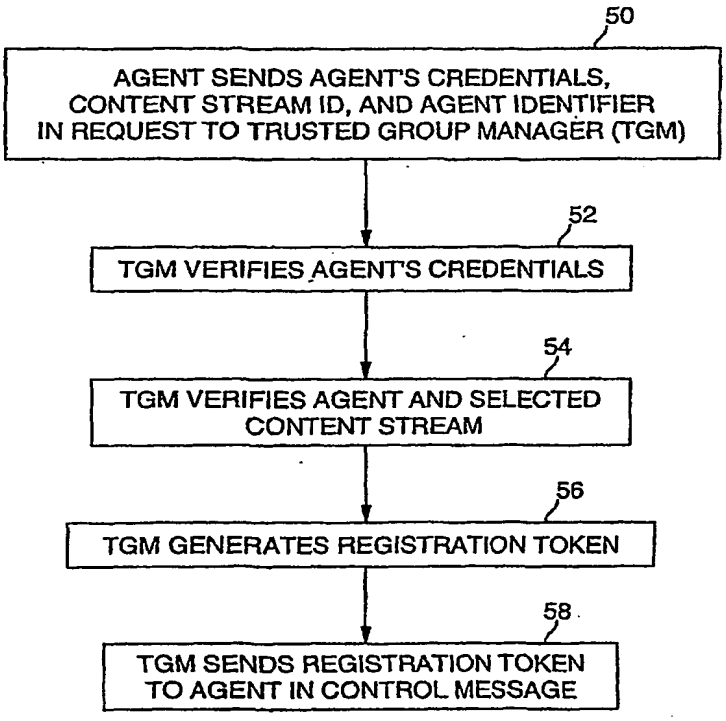

50
AGENT SENDS AGENT'S CREDENTIALS, CONTENT STREAM ID, AND AGENT IDENTIFIER IN REQUEST TO TRUSTED GROUP MANAGER (TGM)
52
TGM VERIFIES AGENT'S CREDENTIALS
54
TGM VERIFIES AGENT AND SELECTED CONTENT STREAM
56
TGM GENERATES REGISTRATION TOKEN
58
TGM SENDS REGISTRATION TOKEN TO AGENT IN CONTROL MESSAGE

Figure 2

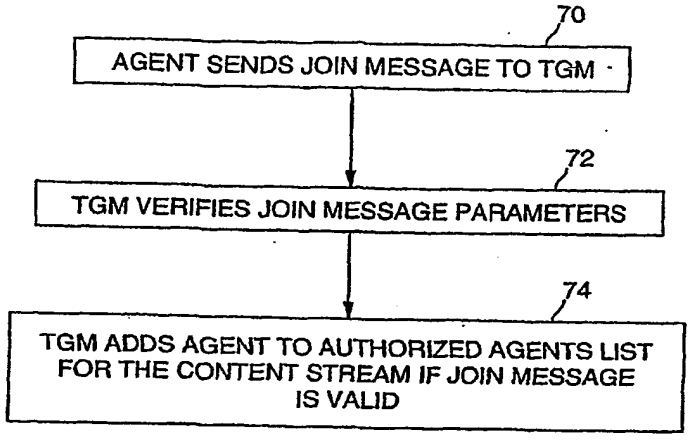


Figure 3

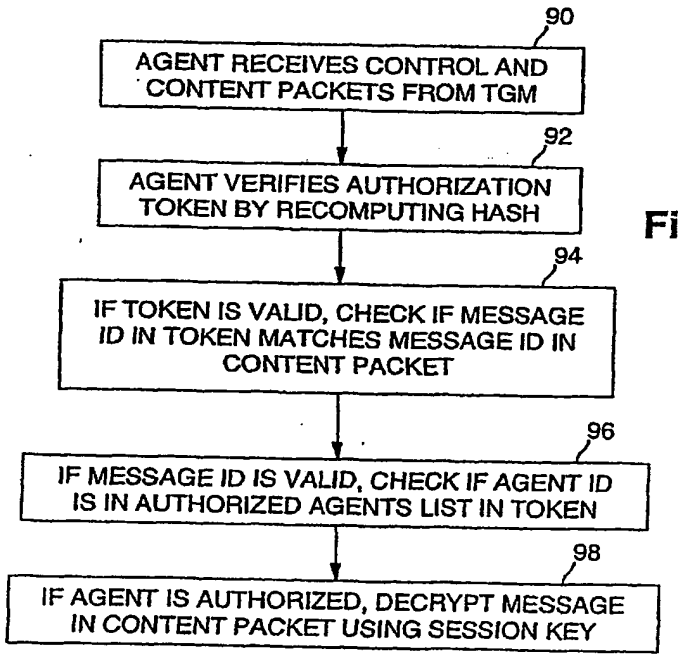


Figure 4

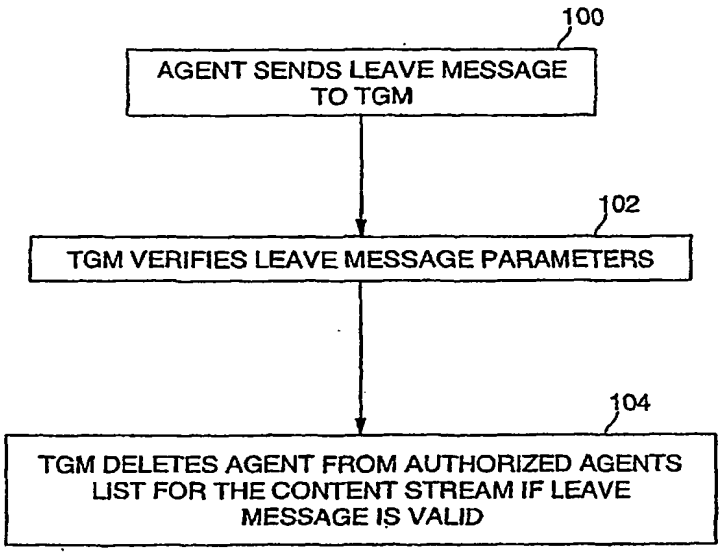

100
AGENT SENDS LEAVE MESSAGE TO TGM
102
TGM VERIFIES LEAVE MESSAGE PARAMETERS
104
TGM DELETES AGENT FROM AUTHORIZED AGENTS LIST FOR THE CONTENT STREAM IF LEAVE MESSAGE IS VALID

Figure 5

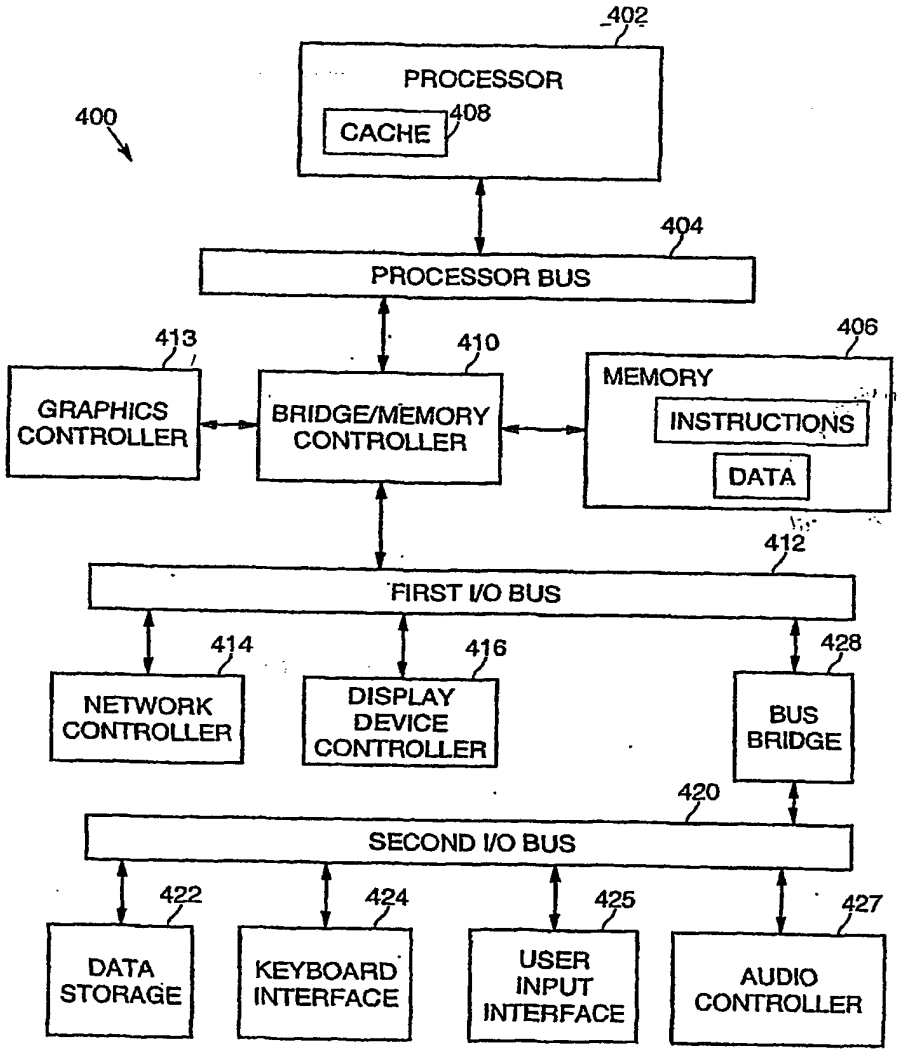


Figure 6

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/001799 A3

(51) International Patent Classification[7]: H04L 12/18, 29/06

(21) International Application Number: PCT/US01/20181

(22) International Filing Date: 26 June 2001 (26.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/603,079 26 June 2000 (26.06.2000) US

(71) Applicant: CONVERA CORPORATION [US/US]; 1921 Gallows Road, Suite 200, Vienna, VA 22182 (US).

(72) Inventor: ROZAS, Carlos, V.; 1534 NW Morgan Lane, Portland, OR 97229 (US).

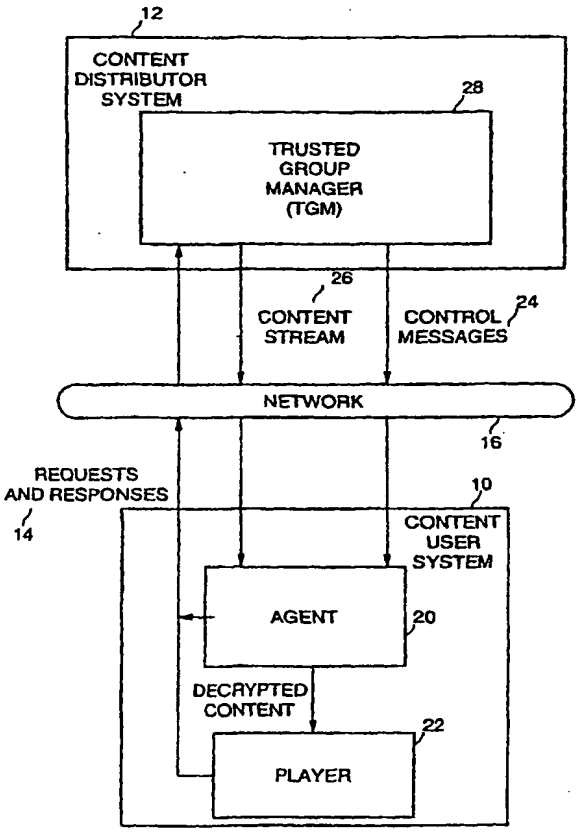
(74) Agents: TALBOT, C., Scott et al.; Cooley Godward LLP, Patent Group, One Freedom Square-Reston Town Center, 11951 Freedom Drive, Reston, VA 20190-5601 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURELY MANAGING MEMBERSHIP IN GROUP COMMUNICATIONS



(57) Abstract: Managing group membership of receivers-in-broadcast and multicast content distribution systems. The invention provides for security in group communications where a single source is broadcasting or multicasting to multiple destination points on a network such as the Internet using a local agent resident on a user system, an authorization token, and a trusted group manager (TGM) representing a content distributor. The local agent may be tamper resistant code providing support for key agreement, decryption, and message authentication functions. The authorization token describes which agents are active and available to decrypt digital content or a per packet basis. The TGM establishes a session key with a group of local agents and generates authorization tokens. The local agent adds and removes itself from a content distribution session (and associated group) based on a series of protocols that do not require a "re-key" for an encrypted content stream being broadcast or multicast by a content distributor. The protocols include operations for registering with a group, joining a group, and leaving a group.

WO 02/001799 A3

Published:
-- *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
11 July 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TERNATIONAL SEARCH REPORT

national Application No
PCT/US 01/20181

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/18 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRISCOE J., FAIRMAN I.: "Nark: Receiver Based Multicast Non-Repudiation and Key Management" ACM CONFERENCE ON ELECTRONIC COMMERCE, 'Online! 3 - 5 November 1999, pages 1-9, XP002198434 Denver, Colorado Retrieved from the Internet: <URL:http://www.labs.bt.com/people/briscorj/projects/charging/content/nark/nark_ec99.pdf> 'retrieved on 2002-05-08! the whole document	1-6, 14-19, 27-31,33
Y		10,12, 23,25
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 May 2002	22/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Mannekens, J

3

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	DUNIGAN TOM, CAO CATHY: "Group Key Management" ORNL/TM-13470, 'Online! 30 September 1998 (1998-09-30), XP002198435 Retrieved from the Internet: <URL:http://www.csm.oml.gov/unigan/gkmp.ps > 'retrieved on 2002-05-08!	10,12, 23,25
A	the whole document	1-36
A	CHI-SUNG LAIH: "On the Design of Conference Key Distribution Systems for the Broadcasting Networks" INFOCOMM 1993, 'Online! vol. 3, 23 March 1993 (1993-03-23) - 1 April 1993 (1993-04-01), pages 1406-1413, XP002198436 San Fransisco, CA, USA Retrieved from the Internet: <URL:http://crypto.ee.ncku.edu.tw/pdf/C18.pdf> 'retrieved on 2002-05-08! page 1409, column 1, line 16 - line 26	1-36
A	US 5 400 403 A (KALISKI JR BURTON S ET AL) 21 March 1995 (1995-03-21) the whole document	1-36
A	WO 97 26611 A (HUGHES AIRCRAFT CO) 24 July 1997 (1997-07-24) the whole document	1-36

TERNATIONAL SEARCH REPORT

Information on patent family members

national Application No
PCT/US 01/20181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5400403 A	21-03-1995	NONE	
WO 9726611 A	24-07-1997	WO 9726611 A1	24-07-1997
		AU 6376596 A	11-08-1997
		BR 9610883 A	13-07-1999
		EP 0815526 A1	07-01-1998
		JP 10508457 T	18-08-1998